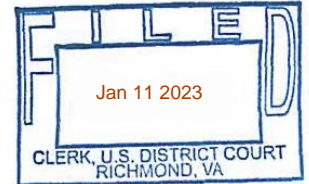


IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division



IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
META PLATFORMS, INC. USER ID:
<https://www.instagram.com/coldheartedlildemon>
THAT IS STORED AT PREMISES
CONTROLLED BY META PLATFORMS,
INC.

Case No. 3:23sw3

FILED UNDER SEAL

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT
FOR STORED ELECTRONIC COMMUNICATIONS**

I, Danielle Shimchick, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for Information associated with Meta Platforms, Inc. User ID <https://www.instagram.com/coldheartedlildemon/> (the "SUBJECT ACCOUNT") that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. ("Meta Platforms, Inc." or "the Provider"), a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Meta Platforms, Inc. to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the user ID. The items to be seized are described in the following paragraphs and in Attachment B.

2. I am a Deputy United States Marshal with the United States Marshals Service and have been since November 2009. During my tenure with the U.S. Marshals Service, one of my primary duties has been the investigation of the whereabouts of federal and local fugitives. Based on my training and experience, fugitives routinely use Meta Platforms, Inc. and social media accounts even while on fugitive status. Fugitives will typically communicate with friends via posts or Meta Platforms, Inc. messenger and disclose personal information regarding their whereabouts. Fugitives will often change the privacy settings to more restrictive means, to prevent law enforcement or other members of the public accessing their page. Throughout my career, I have learned access to Meta Platforms, Inc. must be granted through an internet service provider (ISP) connection. Access to an ISP can be obtained through various means such as telephone lines, fiber optics, television cable and wireless Ethernet (wi-fi). Home ISP is generally obtained and paid for by family/friends to which the fugitive has access to the ISP. Typically, the ISP has location data, which would determine a precise location for fugitive's whereabouts.

3. Additionally, access to Meta Platforms, Inc. through wi-fi will show the general location of the fugitive's whereabouts. As part of the USMS efforts to locate and arrest Cody Dallas GARCIA ("GARCIA"), investigators need to obtain identifying information of the fugitive's Meta Platforms, Inc. page and communications sent to or from the account associated with the subscriber. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. I respectfully submit there is probable cause to believe that evidence, fruits, and instrumentalities of a violation of Unlawful Flight to Avoid Prosecution (18 U.S.C. § 1073), as described in Attachment B, may be located in the SUBJECT ACCOUNT, as described in Attachment A.

RELEVANT STATUTORY PROVISION

5. **Unlawful (or Interstate) Flight to Avoid Prosecution** (18 U.S.C. § 1073) prohibits the interstate travel of a person with the intent to avoid prosecution, or custody or confinement after a conviction, under the law of the state from which that person has fled.

BACKGROUND CONCERNING META PLATFORMS, INC.

6. Meta Platforms, Inc. owns and operates a free-access social networking website of the same name that can be accessed at <http://www.Meta.com>. Meta Platforms, Inc. allows its users to establish accounts with Meta Platforms, Inc., and users can then use their accounts to share written news, photographs, videos, and other information with other Meta Platforms, Inc. users, and sometimes with the general public.

7. Meta Platforms, Inc. asks users to provide basic contact and personal identifying information to Meta Platforms, Inc., either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Meta Platforms, Inc. passwords, Meta Platforms, Inc. security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Meta Platforms, Inc. also assigns a user identification number to each account.

8. Meta Platforms, Inc. users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Meta Platforms, Inc. assigns a group identification number to each group. A Meta Platforms, Inc. user can also connect directly with individual Meta Platforms, Inc. users by sending each user a “Friend Request.” If the recipient of a “Friend Request” accepts the request, then the two users will become “Friends” for purposes of Meta Platforms, Inc. and can exchange communications or view information about each other. Each Meta Platforms, Inc. user’s account includes a list of that user’s “Friends” and a “News Feed,” which highlights information about the user’s “Friends,” such as profile changes, upcoming events, and birthdays.

9. Meta Platforms, Inc. users can select different levels of privacy for the communications and information associated with their Meta Platforms, Inc. accounts. By adjusting these privacy settings, a Meta Platforms, Inc. user can make information available only to himself or herself, to particular Meta Platforms, Inc. users, or to anyone with access to the Internet, including people who are not Meta Platforms, Inc. users. A Meta Platforms, Inc. user can also create “lists” of Meta Platforms, Inc. friends to facilitate the application of these privacy settings. Meta Platforms, Inc. accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Meta Platforms, Inc.

10. Meta Platforms, Inc. users can create profiles that include photographs, lists of personal interests, and other information. Meta Platforms, Inc. users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Meta Platforms, Inc. users can also post information about upcoming “events,” such as social occasions, by listing the event’s time,

location, host, and guest list. In addition, Meta Platforms, Inc. users can “check in” to particular locations or add their geographic locations to their Meta Platforms, Inc. posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

11. Meta Platforms, Inc. allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to “tag” (*i.e.*, label) other Meta Platforms, Inc. users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Meta Platforms, Inc.’s purposes, the photos and videos associated with a user’s account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

12. Meta Platforms, Inc. users can exchange private messages on Meta Platforms, Inc. with other users. These messages, which are similar to e-mail messages, are sent to the recipient’s “Inbox” on Meta Platforms, Inc., which also stores copies of messages sent by the recipient, as well as other information. Meta Platforms, Inc. users can also post comments on the Meta Platforms, Inc. profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Meta Platforms, Inc. has a Chat feature that allows users to send and receive instant messages through Meta Platforms, Inc. These chat communications are stored in the chat history for the account. Meta Platforms, Inc.

also has a Video Calling feature, and although Meta Platforms, Inc. does not record the calls themselves, it does keep records of the date of each call.

13. If a Meta Platforms, Inc. user does not want to interact with another user on Meta Platforms, Inc., the first user can “block” the second user from seeing his or her account.

14. Meta Platforms, Inc. has a “like” feature that allows users to give positive feedback or connect to particular pages. Meta Platforms, Inc. users can “like” Meta Platforms, Inc. posts or updates, as well as webpages or content on third-party (*i.e.*, non-Meta Platforms, Inc.) websites. Meta Platforms, Inc. users can also become “fans” of particular Meta Platforms, Inc. pages.

15. Meta Platforms, Inc. has a search function that enables its users to search Meta Platforms, Inc. for keywords, usernames, or pages, among other things.

16. Each Meta Platforms, Inc. account has an activity log, which is a list of the user’s posts and other Meta Platforms, Inc. activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Meta Platforms, Inc. page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Meta Platforms, Inc. page. Meta Platforms, Inc. Notes is a blogging feature available to Meta Platforms, Inc. users, and it enables users to write and post notes or personal web logs (“blogs”), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

17. The Meta Platforms, Inc. Gifts feature allows users to send virtual “gifts” to their friends that appear as icons on the recipient’s profile page. Gifts cost money to purchase, and a

personalized message can be attached to each gift. Meta Platforms, Inc. users can also send each other “pokes,” which are free and simply result in a notification to the recipient that he or she has been “poked” by the sender.

18. Meta Platforms, Inc. also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

19. In addition to the applications described above, Meta Platforms, Inc. also provides its users with access to thousands of other applications (“apps”) on the Meta Platforms, Inc. platform. When a Meta Platforms, Inc. user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

20. Meta Platforms, Inc. uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Meta Platforms, Inc. user identification numbers; groups and networks of which the user is a member, including the groups’ Meta Platforms, Inc. group identification numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Meta Platforms, Inc. applications.

21. Meta Platforms, Inc. also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Meta Platforms, Inc., including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a

user views a Meta Platforms, Inc. profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from which IP address the user did so.

22. Social networking providers like Meta Platforms, Inc. typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Meta Platforms, Inc. users may communicate directly with Meta Platforms, Inc. about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta Platforms, Inc. typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

23. In my training and experience, I have learned that social networking providers like Meta Platforms, Inc. typically keep records that can reveal multiple Meta Platforms, Inc. accounts accessed from the same electronic device, such as the same computer or mobile phone, including accounts that are linked by "cookies," which are small pieces of text sent to the user's Internet browser when visiting websites. This warrant requires Meta Platforms, Inc. to identify any other accounts accessed by the same browser that accessed the SUBJECT ACCOUNT described in Attachment A, including accounts linked by cookies, recovery or secondary email address, or telephone number. This warrant asks that Meta Platforms, Inc. identify such accounts and produce associated subscriber information.

24. According to Meta Platforms, Inc.’s current Data Policy, which is publicly available on the Internet, Meta Platforms, Inc. also collects other device information, including information from or about the computers, phones, or other devices where the user installed or accessed Meta Platforms, Inc.’s Services, attributes such as the operating system, hardware version, device settings, file and software names and types, battery and signal strength, and device identifiers. Meta Platforms, Inc.’s Data Policy also states that it collects device locations, including specific geographic locations, such as through GPS, Bluetooth, or WiFi signals, as well as connection information such as the name of the user’s mobile operator or ISP, browser type, language and time zone, mobile phone number and IP address.

25. Furthermore, Meta Platforms, Inc.’s Data Policy indicates that it collects information from websites and apps that use Meta Platforms, Inc.’s Services, such as information collected by Meta Platforms, Inc. when the user of an account visits or uses third-party websites and apps that use Meta Platforms, Inc.’s Services, including information about the websites and apps the user visited, the user’s use of Meta Platforms, Inc.’s Services on those websites and apps, as well as information the developer or publisher of the app or website provides to the user or to Meta Platforms, Inc.

26. As explained herein, information stored in connection with a Meta Platforms, Inc. account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Meta Platforms, Inc. user’s “Neoprint,” IP log, stored electronic communications, and other data retained by Meta Platforms, Inc., can indicate who has used or controlled the Meta

Platforms, Inc. account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Meta Platforms, Inc. account at a relevant time. Further, Meta Platforms, Inc. account activity can show how and when the account was accessed or used. For example, as described herein, Meta Platforms, Inc. logs the IP addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Meta Platforms, Inc. access, use, and events relating to the crime under investigation. Additionally, Meta Platforms, Inc. builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Meta Platforms, Inc. “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Meta Platforms, Inc. account owner. Last, Meta Platforms, Inc. account activity may provide relevant insight into the Meta Platforms, Inc. account owner’s state of mind as it relates to the offense under investigation. For example, information on the Meta Platforms, Inc. account may indicate the owner’s motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

27. Therefore, the computers of Meta Platforms, Inc. are likely to contain all the material described above, including stored electronic communications and information

concerning subscribers and their use of Meta Platforms, Inc., such as account access information, transaction information, and other account information.

PROBABLE CAUSE

28. On January 22, 2018, the Lunenburg County Sheriff's Office received information from the Lunenburg Department of Social Services in reference to a sexual assault that occurred earlier in the day. Cody Dallas GARCIA (a juvenile at the time) was alleged to have taken a two-year-old child ("V1") into GARCIA's bedroom, and then proceeded to kiss and touch V1's buttocks area. V1 stated to a caretaker that GARCIA had touched V1's "CooCoo," and pointed to the vaginal area. V1 was transported to the MCV hospital, and a Physical Evidence Recovery Kit (PERK) exam was completed. GARCIA was charged with aggravated sexual battery, arrested by Lunenburg County Sheriff's Office, and transported to Piedmont Juvenile Detention Center.

29. Pursuant to a plea agreement dated March 8, 2018, GARCIA plead guilty to aggravated sexual battery, in violation of Virginia Code Section 18.2-67.3. On April 5, 2018, GARCIA was sentenced in Lunenburg Juvenile Relations Court. GARCIA received a probationary sentence, which included the following conditions: submit to a psycho-sexual evaluation, remain on good behavior for a period of ten years, submit to supervised probation for an indefinite period of time, provide notification of change of address for five years, submit to a search and seizure for five years, prohibited from possessing a firearm/ammunition, prohibited from contact with the victim / mother / siblings / immediate family members for ten years, forbidden from loitering, prohibited from being alone with any children under the age of

eighteen years without adult supervision for ten years, sex offender counseling, and comply with sex offender requirements as required by Probation and Virginia State Police.

30. GARCIA was categorized as a Tier III offender and required to re-register and verify his change of address every three months with the Virginia State Police Sex Offender Registry.

31. On August 25, 2022, the Lunenburg Circuit Court ordered GARCIA placed on GPS location monitoring as an additional term of probation. On November 6, 2022, GARCIA cut his GPS ankle monitor and absconded from probation.

32. On December 18, 2022, three warrants were issued in Lunenburg General District Court, each charging Cody Dallas GARCIA with Failure to Register, in violation of Virginia Code Section 18.2-472.1. The warrants provide surrounding state extradition. The warrants were adopted by the United States Marshals Service Capital Area Regional Fugitive Task Force (“CARFTF”) on January 6, 2022, and assigned to DUSM Danielle SHIMCHICK for fugitive apprehension.

33. On December 25, 2022, GARCIA was involved in a breaking and entering in Mecklenburg County, VA. On December 26, 2022, GARCIA sold what appears to be three phones at the EcoATM Walmart at 200 N. Cooper Drive, Henderson, North Carolina (as part of that transaction, GARCIA was required to provide his driver’s license). According to a confidential source familiar with GARCIA (“CS-1), GARCIA has associates in North Carolina.

34. A search of the NC Sex Offender Registry yielded negative results for GARCIA.

35. GARCIA’s last known location was in Henderson, North Carolina; his current whereabouts are unknown.

36. CS-1 indicated GARCIA has a Meta Platforms, Inc. account under the user ID “coldheartedlildemon.” An open-source search reveals the account as <https://www.instagram.com/coldheartedlildemon> - that is, the SUBJECT ACCOUNT. Your affiant has become familiar with GARCIA’s physical appearance, and recognizes a profile photo displayed for this account as being a photograph of GARCIA. The biography section for the profile lists “19” as being the account-holder’s age. Your affiant is aware that GARCIA is in fact 19-years-old. A post dated March 22, 2022, displays a photograph with GARCIA in the background. The post displays a question – “What color is your soul?” – and a follow-on response: “Red” and “Dallas, you’ve been through more pain than people think of but you never gave up. Despite everything you’ve been through, you’ve remained strong and unbreakable. You are beautiful to watch, but dangerous to mess with.” GARCIA responded to this post with “100% facts.” Your affiant is aware that “Dallas” is Cody GARCIA’s middle name.

37. On January 6, 2022, DUSM SHIMCHICK observed a live video posted from the SUBJECT ACCOUNT. Your affiant recognized GARCIA in the video, in which GARCIA was observed drinking a Four Loko drink and speaking with an unknown individual.

38. GARCIA likely has knowledge of the outstanding state arrest warrant and is evading arrest. As part of the USMS efforts to locate and eventually arrest GARCIA, investigators need to obtain pertinent information regarding GARCIA’s whereabouts, and associates who may be aiding him. Fugitives often use social media as a means of communication with associates through Messenger, direct messages and commenting on other profile pages. Fugitives frequently document their whereabouts on “reels” which may only be viewed for a limited time. Obtaining social media information from GARCIA’s account will

allow investigators to gain further intelligence regarding GARCIA's criminal activity, social circle, identify whom he may be residing with, and ultimately pinpoint his whereabouts.

39. Based upon this investigator's investigative experience, the applicant believes that from the Information gained from the SUBJECT ACCOUNT, a past and current location can be developed for GARCIA.

JURISDICTION AND AUTHORITY TO ISSUE THE WARRANT

40. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the Provider, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

41. A search warrant under § 2703 may be issued by "any district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

42. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

REVIEW OF THE INFORMATION OBTAINED PURSUANT TO THE WARRANT

43. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Meta Platforms, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

44. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrant requested herein will be transmitted to the Provider, which shall be directed to produce a digital copy of any responsive records to law enforcement personnel within 30 days from the date of service. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the electronically-stored information and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, and outside technical experts under government control) will retain the records and review them for evidence, fruits, and instrumentalities of the SUBJECT OFFENSES as specified in Attachment B to the proposed warrant.

45. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the SUBJECT OFFENSES, including but not limited to undertaking a cursory inspection of all messages within the SUBJECT ACCOUNT.

This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails or other electronic communications, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords for which an agent is likely to search.

CONCLUSION

46. Based on the foregoing, I submit that there is probable cause to search the SUBJECT ACCOUNT described in Attachment A for the items described in Attachment B, and I therefore respectfully request that the Court issue the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.

47. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Because the warrant will be served on Meta Platforms, Inc., who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Danielle Shimchick
Deputy U.S. Marshal
U.S. Marshal Service

Subscribed and attested to me by the affiant in accordance with the requirements of Fed. R. Crim. Pro. 4.1 by telephone this 11th day of January 2023.

/s/



Hon. Mark R. Colombell
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
META PLATFORMS, INC. USER ID:
<https://www.instagram.com/coldheartedlildemon>
THAT IS STORED AT PREMISES
CONTROLLED BY META PLATFORMS,
INC.

Case No. 3:23sw3

FILED UNDER SEAL

ATTACHMENT A

Property to be searched

This warrant applies to information associated with the **Meta Platforms, Inc. User ID:**
<https://www.instagram.com/coldheartedlildemon> (the “SUBJECT ACCOUNT”) that is stored at
premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a company
headquartered in Menlo Park, California.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
META PLATFORMS, INC. USER ID:
<https://www.instagram.com/coldheartedlildemon>
THAT IS STORED AT PREMISES
CONTROLLED BY META PLATFORMS,
INC.

Case No. _____

FILED UNDER SEAL

ATTACHMENT B

Particular things to be seized

I. Information to be disclosed by Meta Platforms, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta Platforms, Inc. (“Meta Platforms, Inc.”), including any messages, records, files, logs, or information that have been deleted but are still available to Meta Platforms, Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta Platforms, Inc. is required to disclose the following information to the government for the SUBJECT ACCOUNT listed in Attachment A from August 1, 2022 to the present:

- (a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Meta Platforms, Inc. passwords, Meta Platforms, Inc. security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;
- (b) All address books uploaded, synched, or imported with/to the account;
- (c) All records of Meta Platforms, Inc. searches performed by the account;

- (d) All deleted content associated with the account if still available or stored by Meta Platforms, Inc.;
- (e) All activity logs for the account and all other documents showing the user's posts and other Meta Platforms, Inc. activities, such as content viewed or engaged with;
- (f) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;
- (g) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Meta Platforms, Inc. user identification numbers; groups and networks of which the user is a member, including the groups' Meta Platforms, Inc. group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Meta Platforms, Inc. applications;
- (h) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, deleted messages if still retained by Meta Platforms, Inc., and pending "Friend" requests;
- (i) All "check ins" and other location information;
- (j) All IP logs, including all records of the IP addresses that logged into the account;
- (k) All records of the account's usage of the "Like" feature, including all Meta Platforms, Inc. posts and all non-Meta Platforms, Inc. webpages and content that the user has "liked";
- (l) All information about the Meta Platforms, Inc. pages that the account is or was a "fan" of;

- (m) All past and present lists of friends created by the account;
- (n) All login and logout records relating to the account;
- (o) All information about the user's access and use of Meta Platforms, Inc. Marketplace;
- (p) The types of service utilized by the user;
- (q) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (r) All privacy settings and other account settings, including privacy settings for individual Meta Platforms, Inc. posts and activities, and all records showing which Meta Platforms, Inc. users have been blocked by the account;
- (s) All records pertaining to communications between Meta Platforms, Inc. and any person regarding the user or the user's Meta Platforms, Inc. account, including contacts with support services and records of actions taken;
- (t) Device information, including information from or about the computers, phones, or other devices where the user installed or accessed Meta Platforms, Inc.'s Services, attributes such as the operating system, hardware version, device settings, file and software names and types, battery and signal strength, and device identifiers;
- (u) Device locations, including specific geographic locations, such as through GPS, Bluetooth, or WiFi signals;
- (v) Connection information such as the name of the user's mobile operator or ISP, browser type, language and time zone, mobile phone number and IP address;
- (w) Information from websites and apps that use Meta Platforms, Inc.'s Services, such as information collected by Meta Platforms, Inc. when the user of the account listed in Attachment A visited or used third-party websites and apps that use Meta Platforms,

Inc.'s Services, including information about the websites and apps the user visited, the user's use of Meta Platforms, Inc.'s Services on those websites and apps, as well as information the developer or publisher of the app or website provides to the user or to Meta Platforms, Inc.; and

(x) For all Meta Platforms, Inc. accounts that are linked to or associated with the SUBJECT ACCOUNT listed in Attachment A by machine cookies, secondary or recovery email address or telephone number, provide:

- Names (including subscriber names, user names, and screen names);
- Addresses (including mailing addresses, residential addresses, business addresses, and email addresses);
- Local and long distance telephone connection records;
- Records of session times and durations and IP address history logs;
- Records of login and logout history logs;
- Length of service (including start date) and types of service utilized;
- Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), MSISDN, International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Station Equipment Identities ("IMEI"));
- Other subscriber numbers or identities (including temporarily assigned network addresses and registration IP addresses (including carrier grade natting addresses or ports)); and

- Means and source of payment for such service (including any credit card or bank account number) and billing records.

II. Information to be seized by the government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and outside technical experts under government control) are authorized to review the records produced by Meta Platforms, Inc. in order to locate GARCIA, a person to be arrested pursuant to a federal arrest warrant issued by this district including, for the account listed on Attachment A, information pertaining to the following matters:

- (a) Any information relating to GARCIA's location, including communications about visiting others;
- (b) evidence that can help establish the identity of the SUBJECT ACCOUNT'S user(s), as well as the identities of any individuals providing residence and or aid to GARCIA
- (c) information related to the geographic location of the SUBJECT ACCOUNT'S user(s) and the geographic location of any co-conspirators
- (d) passwords or other information needed to access user's computer or other online accounts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS
PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Meta Platforms, Inc., and my official title is _____. I am a custodian of records for Meta Platforms, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Meta Platforms, Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Meta Platforms, Inc.; and
- c. such records were made by Meta Platforms, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature